ス．製造業　ス社

業務概要	医薬品の製造・販売		
従業員数	約 2,000 人	プライバシーマーク取得	なし
保有個人データ件数	約 43 万件		

１．個人情報に関する概要

（１）保有個人情報件数、種類、利用目的

・製薬会社等で共同利用しているデータベースで利用している保有個人情報数は約 43 万件。
・別途、卸売企業の担当者の個人情報なども保有している。これは同社で独自に管理している。
・製薬会社等共通のデータベースを管理・運用している会社があり、具体的には医師、薬剤師、病院や施設の情報を提供している。医師の氏名や生年月日、最終学歴や、所属病院（同時に複数病院で診療をしている医師もいる)、連絡先などが、提供される情報である。かなりの個人情報が含まれており、製薬会社、薬品卸売会社間で共同利用している。
・共同利用の例として、勤務医が他の病院に移籍したような場合には、その情報を入手した製薬会社の営業担当者がデータベース上で、情報の更新を行う。更新された情報は各社で共有される。
・データベースで蓄積されている情報と、同社で別途取得した情報をマージして使用している。
・保有している個人情報の種類としては、医師、薬剤師等の医療関係者およびアンケート回答者、卸売企業の担当者等の顧客情報を保有している。
・利用目的は同社のホームページに詳細に記載しており、具体的なリストとして誰にでもわかるように提示している。

（２）個人情報保護担当部署

・法務部が担当していている。

（３）個人情報保護管理者の有無、位置づけ

・個人情報保護管理者は「法務部担当取締役」であり、「法務部担当執行役員」が補佐する。
・個人情報保護推進者は法務部長。
・情報管理責任者は各部門長。

・情報システム部門は 14 名であるが、うち、システムがわかるのは 12 名。実際のシステム構築や改修、運用の大部分は外部にアウトソースしている。

（４）認証取得の有無（時期）、認証の種類、その認証を取得した理由・効果

・認証を取得する必要性やメリットが明確でないため取得していない。
・システム開発・改修、運用は外部にアウトソーシングしており、アウトソーシング先はプライバシーマークなどの認証を取得している企業に限って選定している。

（５）個人情報保護に向けた取組経緯

・平成 17 年 4 月 1 日付で個人情報保護規程および個人情報保護マニュアルを制定すると同時に、全社（グループ会社を含む）を対象にした説明会を開催したのが全社的な取組の始まりである。
・現在は、各会議等において適宜指導している。

（６）個人情報の保有・管理・提供等に関する業界等の特徴

・医療関係者情報の共同利用が特徴的である。製薬各社では、かつては医師の個人的な情報（趣味、会談・会食等、家族構成や参加したイベント等）もメモ的に保管していたが、個人情報保護法施行にあわせて、製薬会社間で議論して現在の仕組みを構築することにした。
・製薬会社は卸売会社を通じて病院に薬を販売する際に、VAN や EDI を使って、各社が売上や出荷、注文などの情報を 1 つの大きなシステムの中で共用している。四半世紀前からそのような行動が当たり前になっているので、医療関係情報の共有も抵抗なく実現できている。
・同社の商品をどこの配送センターからどこの卸売会社に出し、どの担当者がどうやって病院に提供したのか、というところまで追えるようになっており、トレーサビリティが確保されている。
・同社では MR（医薬情報担当者）の離職率はそれほど高くなく、離職者に対して特に注意しているようなことはない。取扱製品が特徴的であるということ、日系企業であるということも理由ではないかと思う。

２．個人情報の適切な保護のための取組について

（１）準備（規程・体制づくり）

・コンプライアンスガイドブックを作成して配布している。
・コンプライアンスガイドブックには「どのようなことをしたら、個人情報保護法違反

になるか」ということが具体例を交えて記載されている。本ガイドブックに違背する行為については懲戒処分の対象となることが就業規則に明記されている。

（２）個人情報の取得

・医師は共同利用しているデータベースに自分の個人情報が掲載されることについては、オプトアウトできる。

・共同利用しているデータベース入力する情報については、入力の度に医師等から同意を取得しているわけではない。医師もそのようなデータベースに自分の情報が登録されていることを知っており、オプトアウトが可能だからである。

・このデータベースの重要な社会的意義は、「医師や薬剤師などの情報が一元かつ最新に管理されていること」である。その結果、製薬企業は副作用情報を正確に発信することができ、医師、薬剤師等はリアルタイムで副作用情報を受信できるという利益を享受する。

（３）個人情報の利用

・共同利用のデータベースに蓄積されている個人情報と、同社における独自の個人情報をマージして分析等を行っている。

・例えば「売上」などは、薬の種類、病院、施設ごとに売上の分析をしたりしている。そのような分析を行う際に共同利用のデータベースの情報とマージして分析したりしている。マージした情報を活用することで、MR ごと、病院ごと、薬ごとに売上を計算することができるようになっている。

（４）個人情報の管理

①情報の管理体制

・社員証（IC カード）を多目的に利用しており、入室・退室管理や、パソコン等へのアクセスの際の認証に利用している。

・ファイルサーバも各部門で用意しており、重要文書を保存できるようにしている。パソコンの中にデータを残さないようにしている。

・社員証（IC カード）によって、パソコンにログインし、さらに作成したファイルを暗号化できる。

・複数人が使える共用パソコンを使用する際には、情報システム部門の長による承認が必要であり、不用意に共用パソコンが増えないようにしている。共有パソコンの利用状況のログも取っており、一定期間でほとんど利用がない場合には使用許可を取り消し、撤去している。

（ログ取得に注力し、有事に備えている）

・キーボードに至るまで資産管理、ログ取得の対象にしており、詳細に把握している。何かが生じたときに、どうして、どのように生じたのかをトレースできれば良いと考えており、そのためにログを詳細に取得することに注力している。
・ログについては、事象が明らかになった場合に初めてチェックを行う。自動的にログを解析するような仕組みにはしておらず、そこまで実施する余裕はない。
・内部統制対応として、情報システム部門の長であっても各部門のシステムにアクセスすることはできなくした。このため、システム等の改修のために相談があると、アクセスする権限を付与してもらう手続きを経た上で対応する。
・USB メモリも情報システム部門の長による承認がないと使えないようにしている。全面的に使用禁止にしたいのだが、顧客（医師）から USB 経由でデータを渡されるケースは少なくなく、顧客に対して「USB メモリ使用をやめてほしい」、という依頼はできないので、リスクは認めながらも顧客のニーズに配慮して禁止していない。
・DVD-RW は外付けにしている。社員個人には配布しておらず、課長クラスに必要に応じて渡し、課長決裁で使えるようにしている。
・個人が表計算ソフト等で名簿リストなどを作成している場合は、レポジトリ機能を有したアプリケーションを活用して、チェックイン・チェックアウト、バージョン情報について管理ができるようにしている。

（携帯電話のメール送受信の制限による漏えいリスクの低減と利便性をバランス）

・携帯電話は、従来は MR については個人用携帯電話を使用させており、公用の電話のみ、電話番号の頭に特別な番号をつけるだけで、会社が通話料金を自動的に負担するという仕組みで運用していた。
・しかし、携帯電話の紛失によって、個人情報が紛失してしまうリスクが高いため、会社から携帯電話を支給する方式とした。
・支給に際しては、携帯電話からはメールの送受信ができないように設定（ロック）しており、携帯電話から通常のメールは一切できない。
・しかし、メールを全て禁止すると、顧客先を回っている MR の業務遂行には問題が生じるので、特別なアプリケーションを導入して、会社のメールアドレスで受信したメールを携帯電話で閲覧できるようにした。但し、閲覧しかできないようになっており、添付ファイルは見られないようになっているなど一定の制限を課している。
・また、安否確認をする場合のみ、メールが携帯電話に送信されるようになっている。安否確認のメールはサーバ上で「ホワイトリスト」に登録し、メールを送受信できるようにしている。
・上記の仕組みだと、会社に届いたメールを携帯電話で閲覧するためには、アプリケーションを起動しないとメールが届いているのかどうかすらわからないという問題があ

った。そこで、「件名」と「送信元」の情報のみの通知を携帯電話で受信できるようにカスタマイズしてMRの利便性にも配慮した。
・携帯電話の紛失時には、携帯電話会社の汎用サービスであるメモリの消しこみ、GPSによる携帯電話の所在確認を利用している。
・メールの保全がJ-SOX対応で必要であったこともあり、このような対応をした。
・どこに電話をかけたのかということは請求電話明細でわかるようになっているので、ログとしてチェックができるようになっている。
・携帯電話をかける際には、全社統一の番号を入力してロックを解除しないと、電話がかけられないようになっている。このロックは1分ごとに必ずかかるようになっている。これは携帯電話キャリアから求められた対応である。その面倒さに、当初は社員からも不平不満が出たが、1ヶ月程度で慣れた。
・着信と同時に相手を識別できないと顧客である医師に対して失礼にあたる場合があるため、アドレス帳は使えるようにしている。その代わり、遠隔操作でアドレス帳を消去できるようにしている。公衆電話から自分の携帯電話に電話（規定回数）することにより、消去できる。

②従業者への教育方法
・コンプライアンスを目的にアンケートを実施した。従業員は、携帯電話の安全な利活用のためにインフラを整えることや、会社で費用負担をすることについて認識しているようで、「そこまで会社からしてもらっているのだから、その上で違反行為をしたら大きな罰則があって然るべき」という認識を持つ者が多いことは明らかになっている。
・法務部で年1回、全国を回って教育を実施している。営業職が多いので、都道府県単位の集合研修を実施している。毎回ではないが、個人情報保護、情報セキュリティの内容を取り込むようにしている。

③盗難対策
・社内への入室・退室についてはICカードで厳密に管理を行っており、誰がどの部屋にいるか、ということまで管理されるようになっている。

④ノートPCの安全対策
・電源を入れた際に、BIOSでパスワードを入力しないと次に進めないようになっている。
・ハードディスクは暗号化している。
・社員証をリーダーで読み込ませたうえ、各個人に割り当てられたパスワードを入力しないと、パソコンが使用できないようになっている。

⑤外部委託先管理

（社内の各部署の外部委託時には法務部が同行チェックすることで意識付け）

・外部委託に際しては、「個人情報取扱適性判定書」を作成しており、社内規程、管理責任者、第三者認証取得有無、入退室管理、システムセキュリティ、再委託有無・再委託先管理方法、過去の漏えい事故の有無などについて、チェックした上で委託を行う。委託先選定の際には、委託先に立ち入り検査を行い、委託担当部署と法務部が同席した上で実施している。

・立ち入り調査で法務部も一緒に立会いを行うのは、担当部署に対して法務部はしっかりチェックしていることを認識させると同時に、委託先企業に対しては「個人情報に対する意識の高い会社」であることを印象付けるねらいがある。

・委託先企業がプライバシーマークなどの認証を取得している場合には、「認証の更新や評価を受けた」、という報告も毎年確認させてもらうようにしている。

・委託期間中においても、「個人情報取扱報告書」という書式を用意しており、委託先の状況をチェックしている。その他にも、打ち合わせで敢えて先方の会議室を利用させてもらったり、先方の執務室に入らせてもらったりして視察させてもらい、セキュリティの運用について評価している。

⑥日常点検・確認の方策

・特に話は無かった。

⑦初歩的ミスの防止策

・特に話は無かった。

（５）個人情報の消去・破棄

・外部委託しているベンダーがアーカイブログを削除するような場合にも、担当役員の許可を得た上で消去しており、部長決裁だけでは削除もできないようになっている。

（６）個人情報の監査

・内部統制の観点もあり、IT ガバナンス統制全般について、監査法人による外部監査を受けている。

・従来は軽微な不備は指摘されたが、大きな不備は指摘されたことが無い。

（７）苦情処理・顧客対応

・ほとんど苦情などは来ていないし、問題は生じていない。開示請求は過去０件。

（８）事故発生時の対応

・携帯電話は紛失時には情報システム部門の長に連絡することになっている。法務担当執行役員にもすぐ連絡が行くようにしており、スピーディーに対応できるようにしている。社内イントラネットに、紛失時の対応として記載されている。

・普段からアクセスログや操作ログ等を記録して、どこから誰がいつ漏えいしたのか、ということを追跡できるようにするが重要であると考えている。

以　上